

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
 FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST 1976



YES, DON, THERE IS AN ELINT!.....	P.L. 186-36
INITIATIVES IN SIGINT REPORTING.....	4
NOTE ON FRANCOPHONEGLOS.....	6
CLUSTERING OF CRYPTANALYTIC DATA.....	7
NSA'S SYSTEM FOR GRADING TRANSLATIONS.....	9
LANGUAGE IN THE NEWS (FRENCH).....	12
INTEGRATED ANALYSTS FOR ASIA.....	13
RESEARCH IN SPEECH PERCEPTION.....	15
NSA CRYPTOLOGIC COLLECTION.....	17
LETTERS TO THE EDITOR	19

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

Classified by DMRNSA/CHESS (NSA/CSSM 123-2)
 Exempt from GDS, EO 11652, Category 2
 Declassify Upon Notification by the Originator

~~TOP SECRET~~

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. III, No. 8

AUGUST 1976

PUBLISHER

WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (8025s) P.L. 86-36
Language.....Emery W. Tetrault (5236s)
Machine Support.....[redacted] (3321s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Frederic O. Mason, Jr. (4142s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

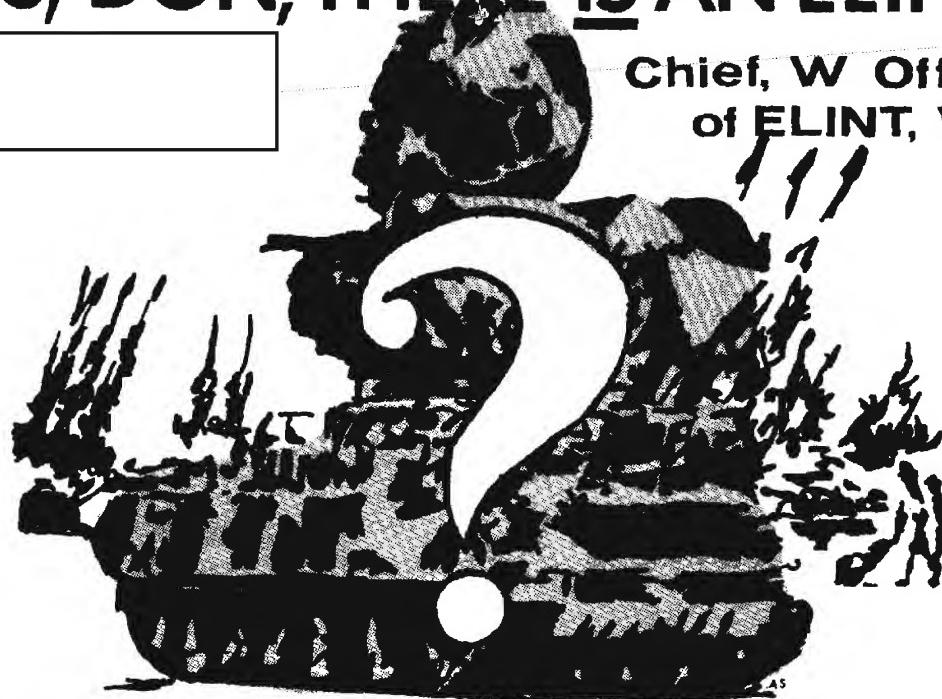
~~SECRET~~

YES, DON, THERE IS AN ELINT!



**Chief, W Office
of ELINT, W2**

P.L. 86-36



EO 1.4. (c)
P.L. 86-36

Yes, Don, there is an ELINT! Because you don't recognize it, doesn't mean it doesn't exist. Your NSA colleagues who plant its seeds, who nurture its growth, who channel its energies, and who harvest its fruits resemble in many ways the more "normal" NSA employee. You might, therefore, have as much difficulty recognizing an ELINTER as you do ELINT, but, believe me, they exist too.

In the April issue of CRYPTOLOG you asked if the real ELINT would stand up.* You indicated that it appears to be a shadowy operation and that many COMINTERS would like to know what it is all about. Happy to oblige. We ELINTers have been so busy practicing our science (art?) that we didn't notice all of you waiting to be enlightened in the ways of ELINT -- perhaps to join the fun. We're a proud bunch who know we are an NSA minority specialty group with an important job to do, and we think that we're doing it rather well. We can do it even better, and we are working at that. We will attempt to throw light into the shadows, remove mystery, and minimize jargon.

Formal definitions of ELINT do in fact include all non-communications electronic emission intelligence except lightning and nuclear emissions. As practiced at NSA, our energies

are devoted primarily to ELINT

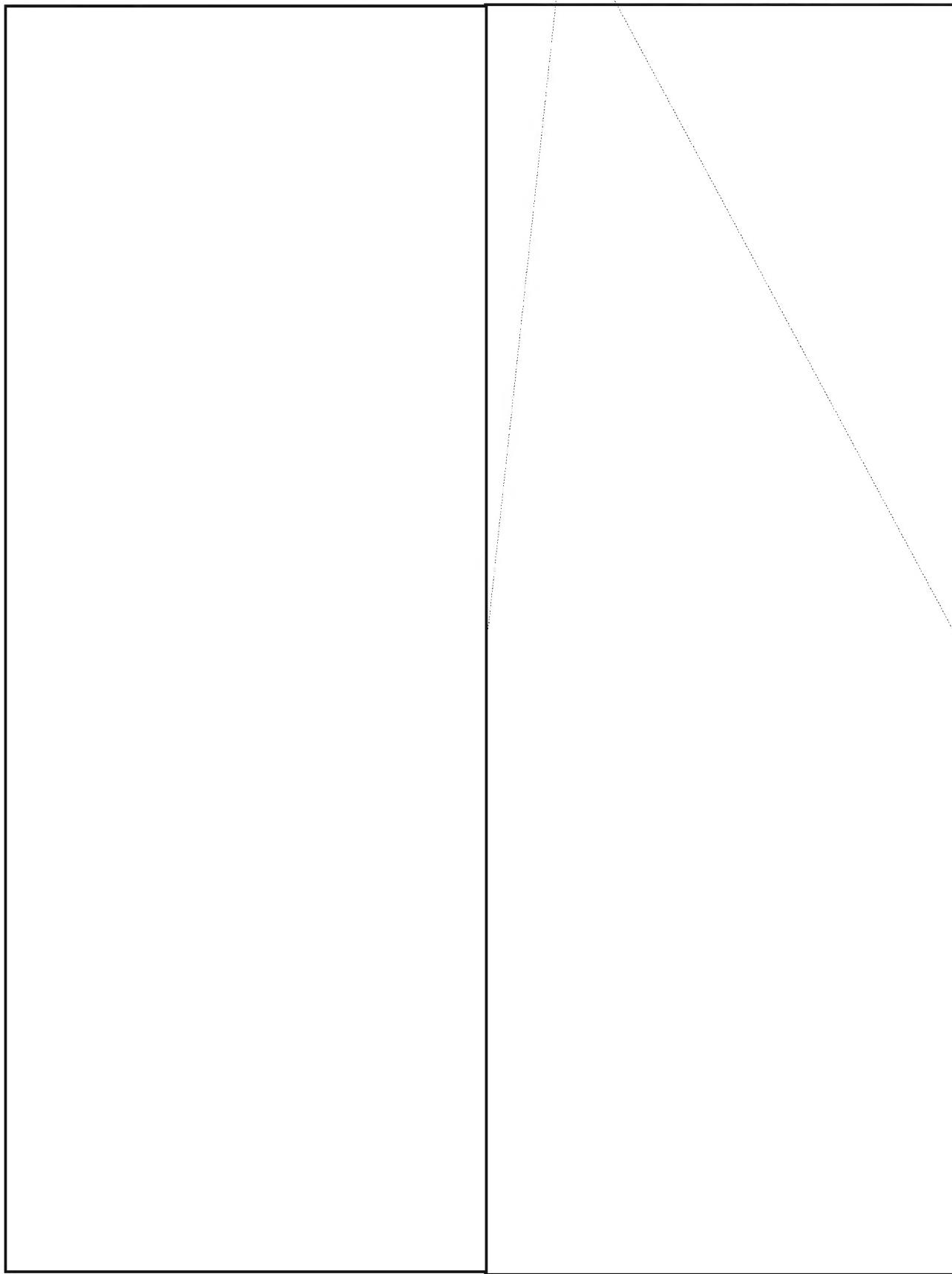
NSA partitions ELINT into two classes:
Operational ELINT and Technical ELINT.

* [REDACTED] "Will the Real ELINT Please Stand Up?", CRYPTOLOG, April 1976, p. 5.

~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

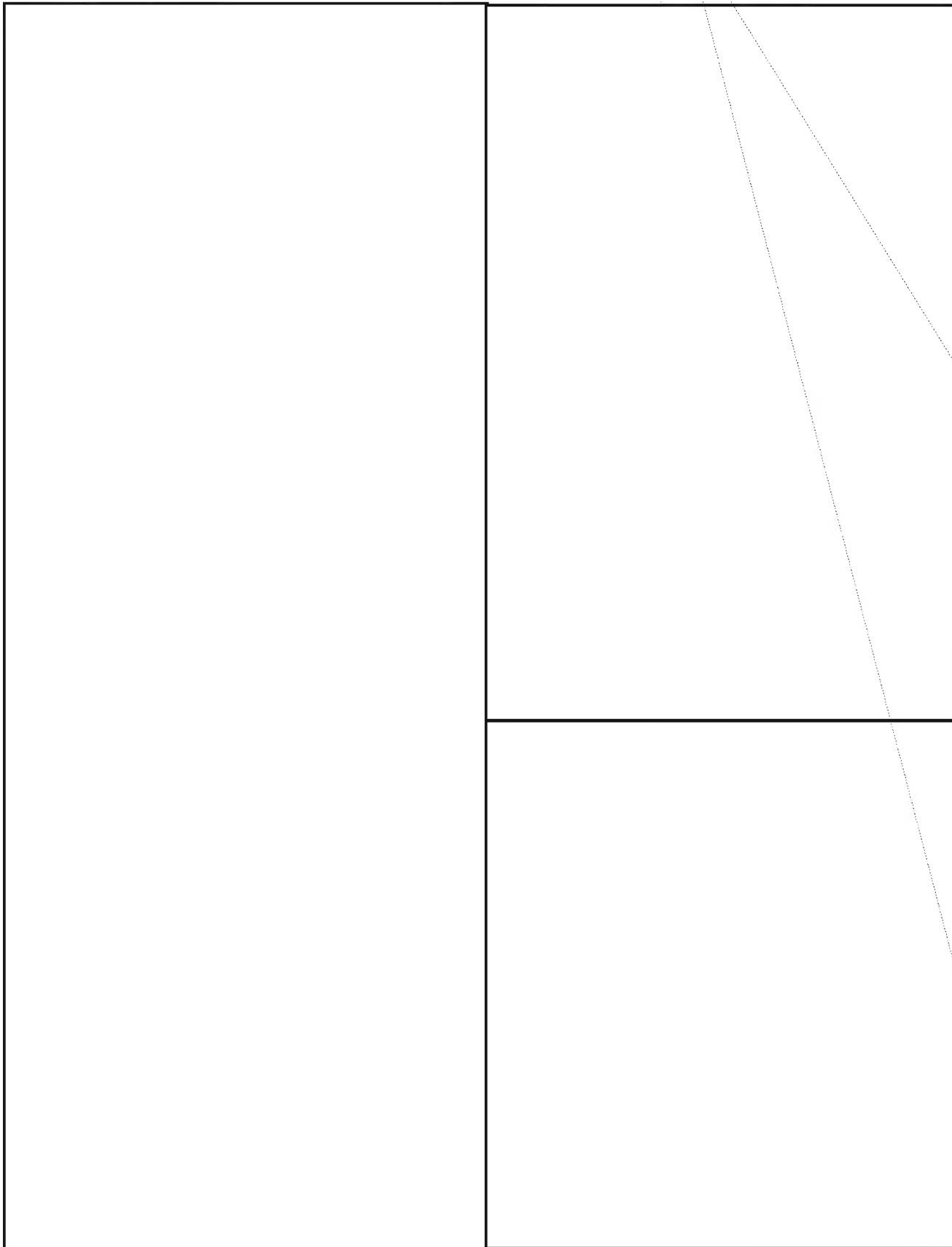
~~SECRET~~

EO 1.4. (c)
P.L. 86-36



~~SECRET~~

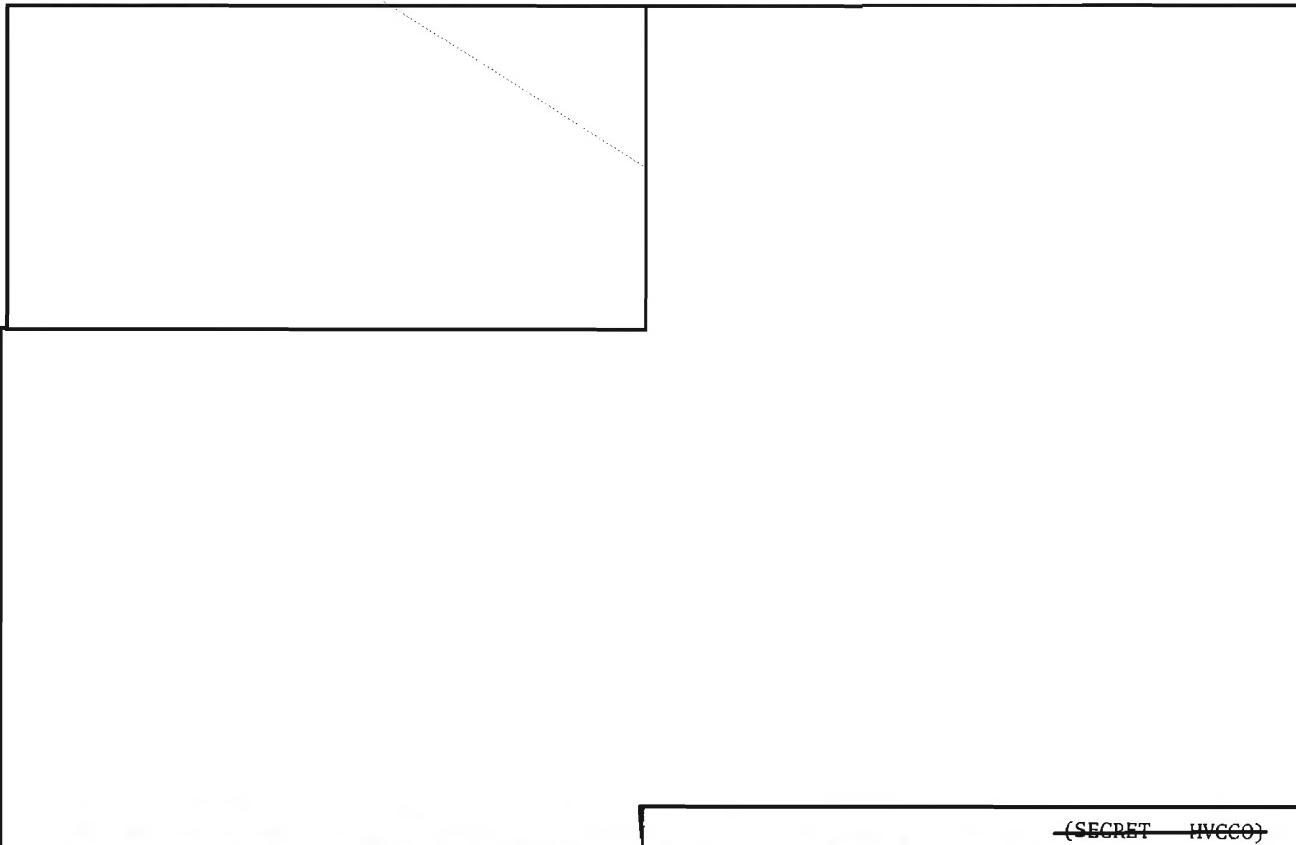
EO 1.4. (c)
P.L. 86-36



August 76 * CRYPTOLOG * Page 3

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

(SECRET HVCCO)

INITIATIVES IN SIGINT REPORTING

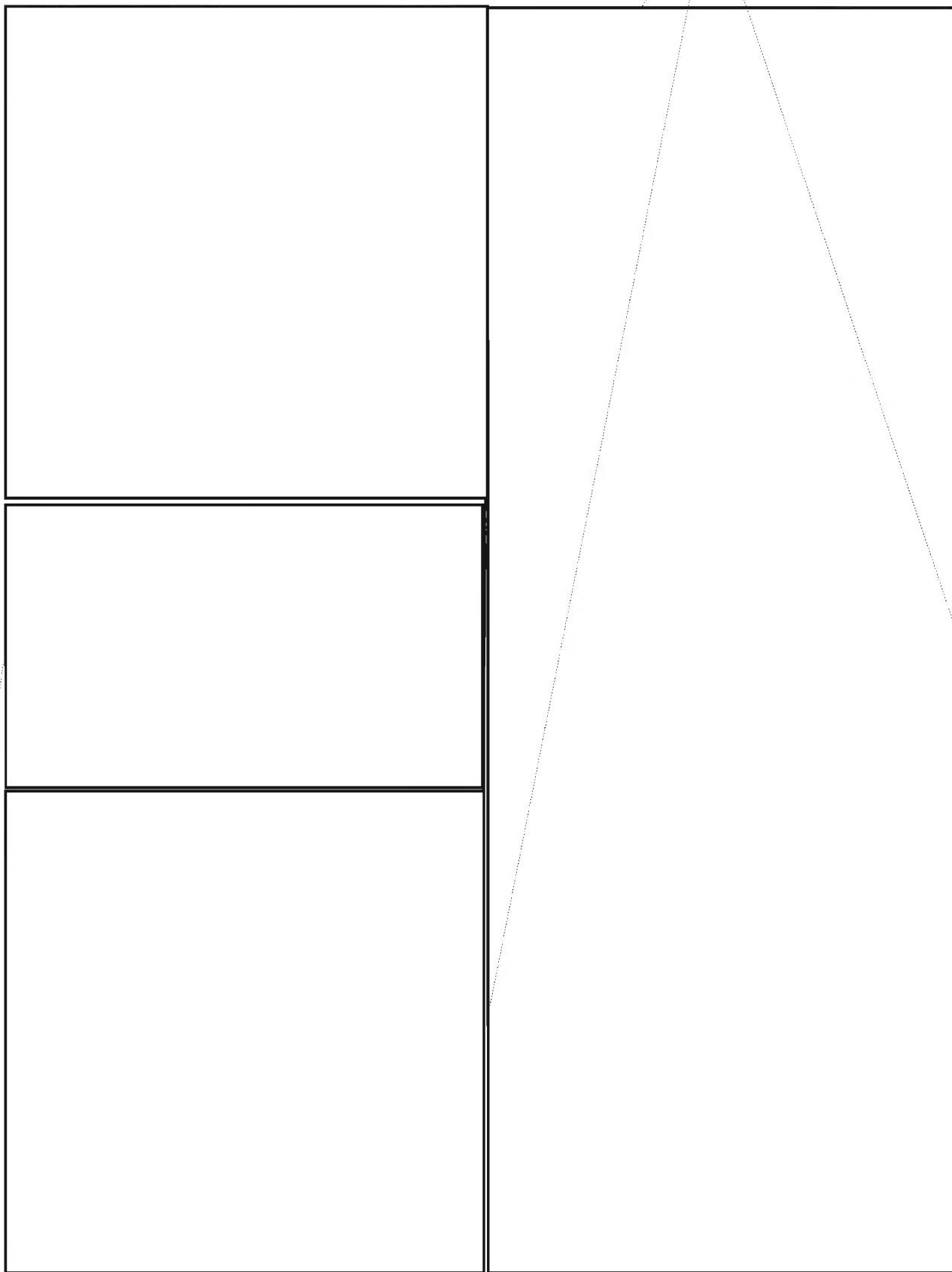
In the last few years the U.S. SIGINT System has been pressured from many directions to improve the utility (access) of SIGINT and, at the same time, to respond to oft-expressed concerns that SIGINT security needs tightening. Thus, on one hand we must provide SIGINT quickly and directly to the levels where it will be useful (in some cases to non indoctrinated recipients); on the other we must scrupulously avoid distribution of product to places where there is no need for it, and, above all, we must not gratuitously reveal the SIGINT "secrets" (sources, methods, techniques). So, by varying degrees of loosening and binding the reporting and distribution procedures, we have made significant modifications which will work toward increasing both the usefulness and security of SIGINT.

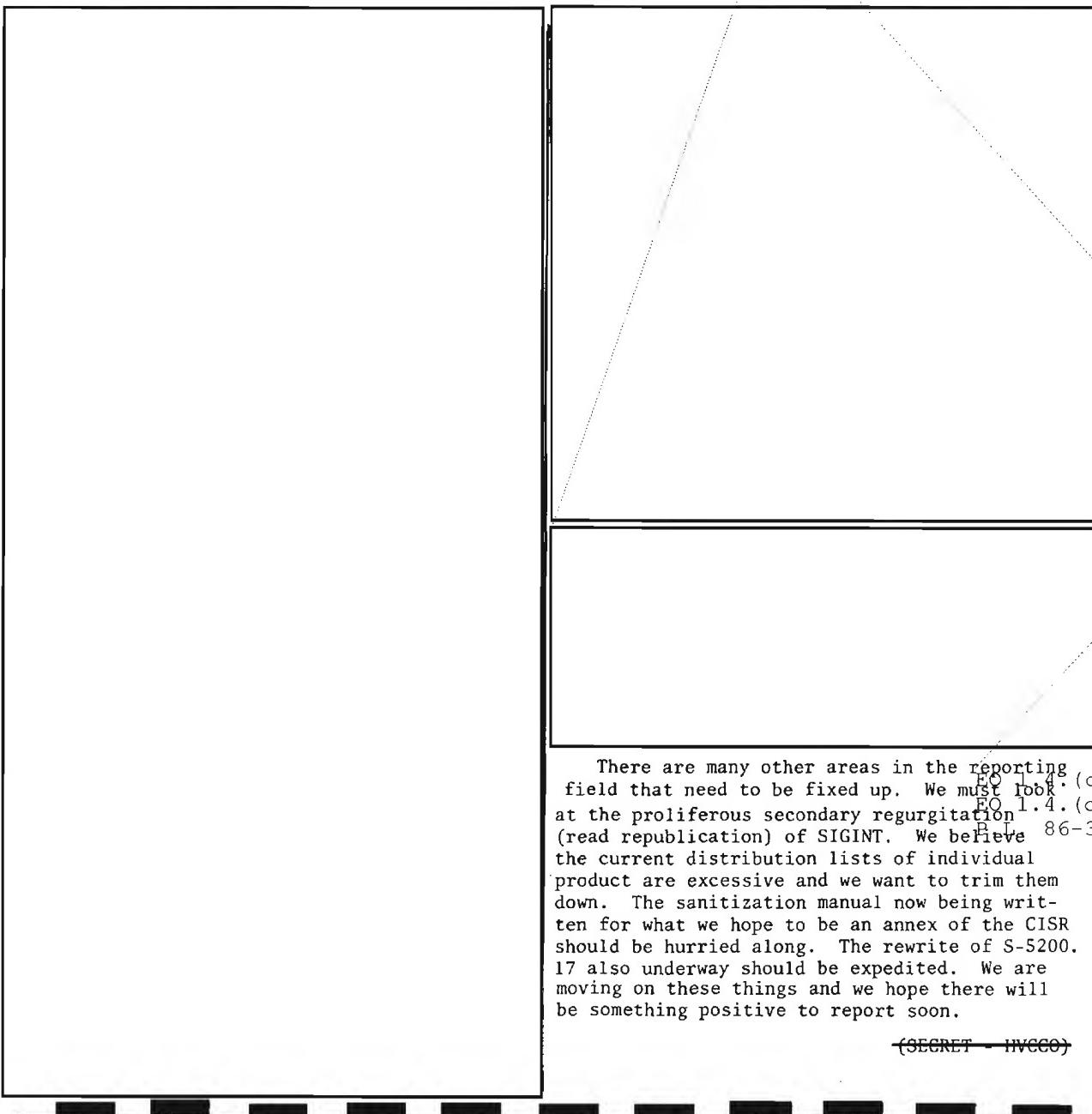
To highlight the key changes which have occurred in the last year or so, let's start

with Subcategory II(X) COMINT reporting. P. Some 86-36 time ago, NSA invented the detach line format as an aid to recipients in implementing the less restrictive Subcategory II(X) COMINT usage provisions of the DCI's Communications Intelligence Security Regulations (CISR). The idea was that the producer would issue this "less sensitive" COMINT at a straight SECRET (non-codeword, non-COMINT channels) classification between two detach lines

~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~



~~SECRET~~EO 1.4. (c)
P.L. 86-36

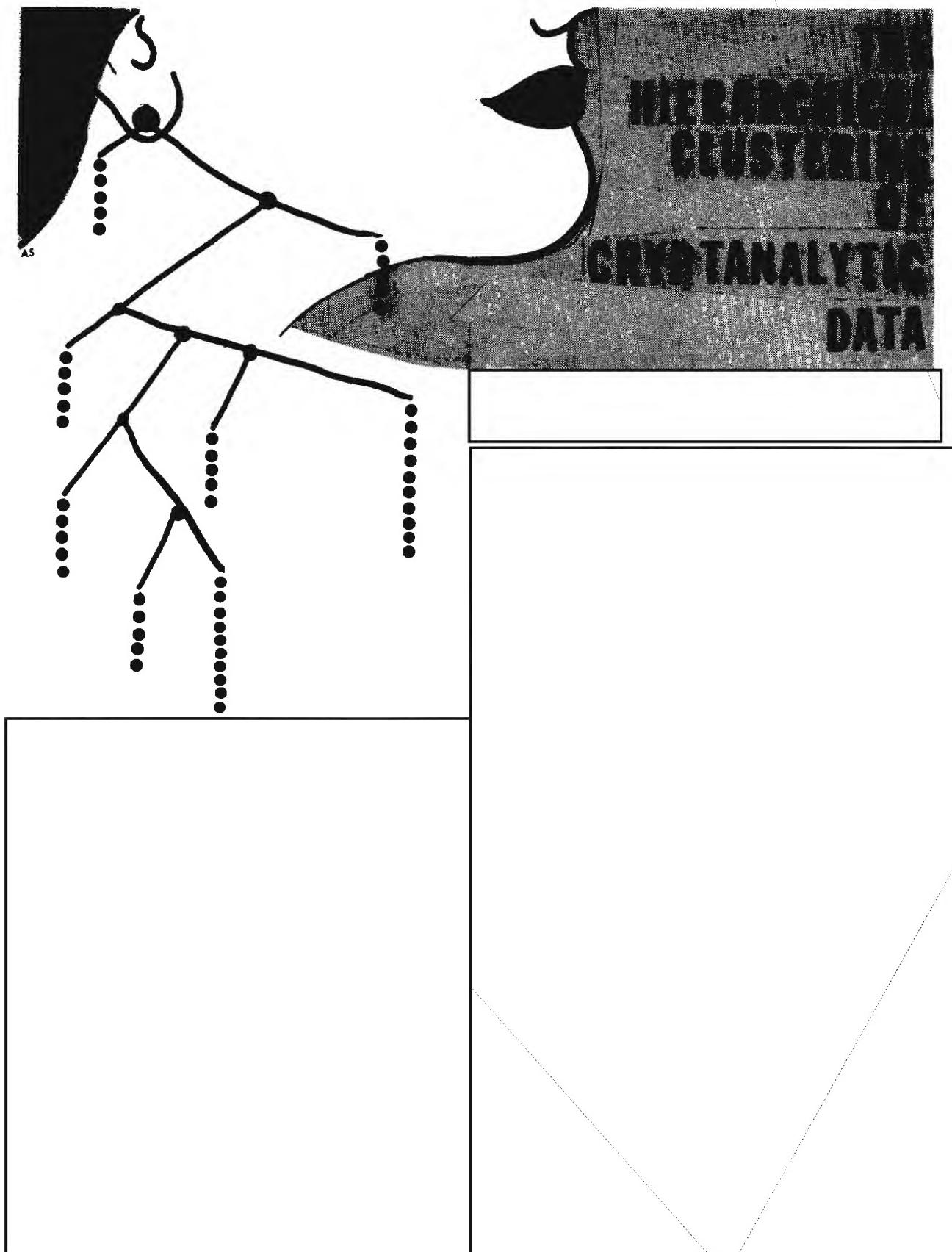
There are many other areas in the reporting field that need to be fixed up. We must look at the proliferous secondary regurgitation (read republication) of SIGINT. We believe the current distribution lists of individual product are excessive and we want to trim them down. The sanitization manual now being written for what we hope to be an annex of the CISR should be hurried along. The rewrite of S-5200. 17 also underway should be expedited. We are moving on these things and we hope there will be something positive to report soon.

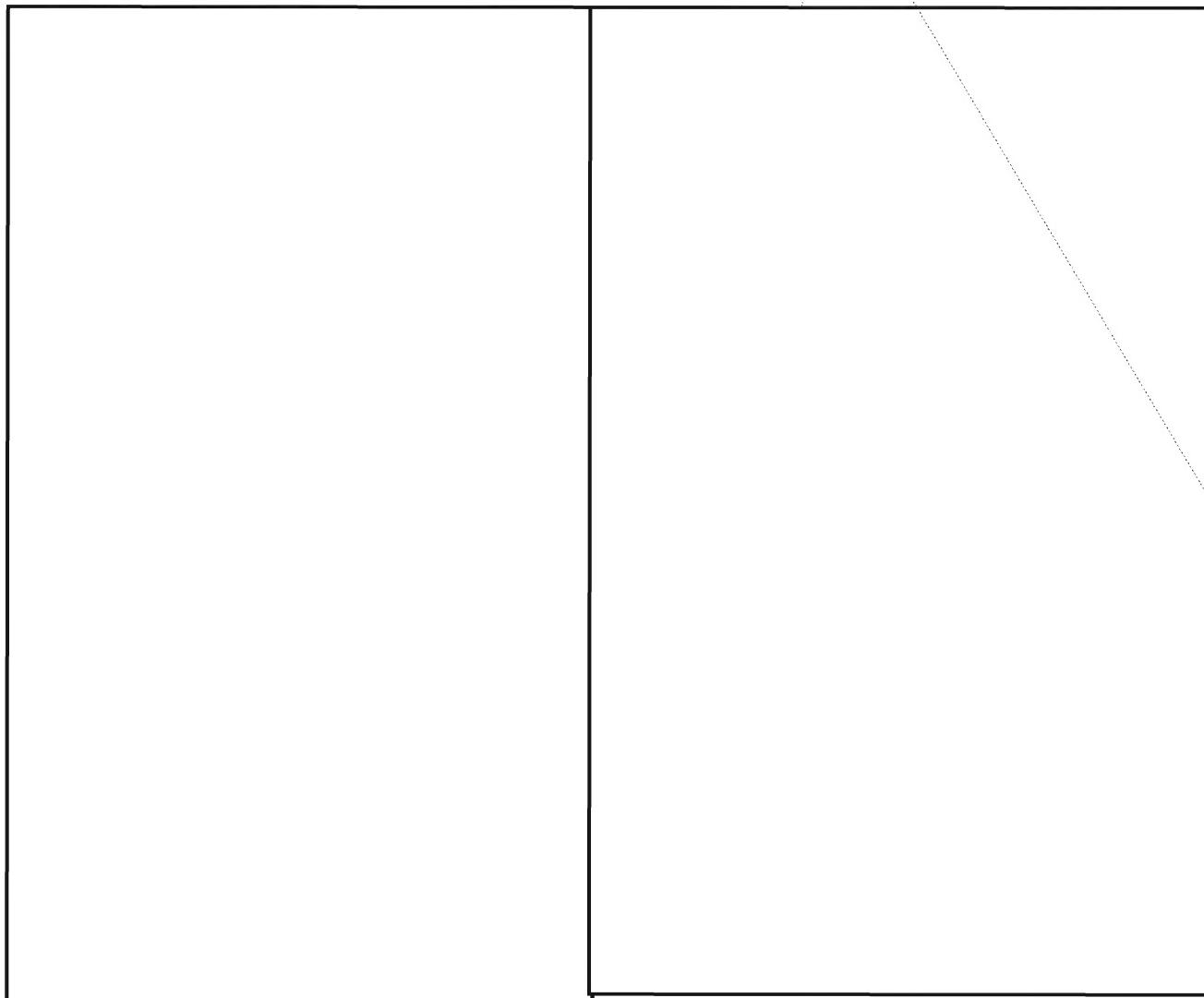
(SECRET - HVCCO)

FPG LIVES!

Barbara Dudley, File Executive of the FRANCOPHONEGLOS computerized dictionary of the French Language (for details, see CRYPTOLOG, October 1975, p. 10), has returned to NSA on a consultant basis. She is training her successor, who will also be available for researching questions and for giving instructions in on-line querying. Phone 4814s or 4707s to make known your critical needs in French-language subject matter, so that the most needed source material can be fed into the computer.

~~(CONFIDENTIAL)~~~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET SPOKE~~~~SECRET SPOKE~~

~~SECRET SPOKE~~~~SECRET SPOKE~~

OH? REALLY??

John Kenneth Galbraith, then United States ambassador to India, was in Toronto to receive an honorary degree. As he recalls it in *Ambassador's Journal* (Houghton Mifflin): "I had asked that a certain cable from Washington to New Delhi be relayed to me through our consulate in Toronto. Consular aides brought the coded message out to me at the airport -- a mass of numbers. There were no facilities for decoding so I asked how they managed. They said when something arrived in code, they phoned Washington and had the original message read to them."

(UNCLASSIFIED)

~~SECRET SPOKE~~

UNCLASSIFIED

NSA'S SYSTEM FOR GRADING TRANSLATIONS



P.L. 86-36

1. Introductory Note

A great deal of language testing in the U.S. government and elsewhere involves setting a passage of some arbitrary length for translation and applying equally arbitrary and often unreliable grading procedures. The wisdom of using the translation vehicle as a method for assessing foreign-language competence is probably questionable, but if this procedure is adopted, it should be applied as consistently and reliably as possible. I describe below the criteria for evaluating translations which we have applied at NSA since early in 1972.

2. Scoring System

Our testing system requires that subjects translate material of nontechnical nature which will generate 500-600 English words. My colleagues and I have set up a scoring system based on 100, and have set 70 as a passing grade. At least two graders, and most often three or four, grade each paper independently, assessing errors according to the system described below. Each paper is studied with great care by each grader in the interest of absolute fairness. Even so, the tendency to read into the text what one would like to see there, plus inevitable disagreement over the exact nature of translation errors, require that the graders compare their results. Agreement on every point is often impossible, since

no two people view the texts of natural languages in exactly the same way. However, final pass/fail judgments are usually made against a spread of no more than 5 points. Thus, it is possible for two graders to award a 70 and a third, 65. As unanimity is not essential, such a paper could pass. Cases of this sort have been infrequent.

2.1 Types of Errors

We have made a three-way distinction among linguistic phenomena which we have found valid and reliable in assessing the errors of beginning translators (this scheme is of little or no value in evaluating the work of experts). The three categories we have distinguished are:

- foreign-language syntax,
- lexicon plus some grammar features of the foreign language, and
- English-language usage and convention.

The first two involve the translator's comprehension of the foreign language and his ability to show his understanding in correct, if unidiomatic, English rendering. The last reflects his skill in not only conveying the meaning of the passage, but doing so in idiomatic English. Four points are taken off for each syntactic error; two points for each lexical error; and one point for poor English usage and violation of convention.

UNCLASSIFIED

UNCLASSIFIED

Below I attempt fuller definitions and examples of the three possible sources of error and follow with some actual instances of poor translation from foreign languages to English. I also explain the rationale for specifying the type of error in cases where analysis may be difficult.

2.2 Syntactic errors (4 points each)

In the English sentences "The dog bit the man" and "The man bit the dog" the words are identical but the meanings are exactly opposite. The element which determines the difference is the positioning, or order, of the words. A native speaker of another language trying to learn English would have to be aware that in this sentence, as in most others, word order is all-important and that failure to appreciate this fact will lead to major error. In the NSA translation-grading system, a test subject making an equivalent error in translating from another language into English would be docked 8 points (for two 4-point errors: subject and object incorrectly identified in relation to the verb).

A second example somewhat more difficult to judge in respect to verb-noun relationships would be "Air filled the balloon" vs. "The balloon was filled with air." If it is clear from context that someone or something was involved in the act of filling the balloon (a mechanic, a pump, etc.), then the two sentences are vastly different, and failure to bring the fact out would cost the translator 4 points. If, however, the phrase "was filled with" is roughly synonymous with "was full of," we would at most take off one point (see below).

The two examples above involve what are called case errors: errors in establishing the true relationship of noun to verb. Below I give some actual examples of case error in translating from Russian to English. The following two examples are taken from a passage dealing with the destruction of a bridge and the need for a new one:

<u>Correct translation</u>	<u>Wrong translation</u>
"In 1943 the Germans blew up the bridge while retreating."	"In 1943 the bridge was blown up during the German retreat."
"The youngsters cross a [makeshift] suspension bridge. Other citizens also use it, risking life and limb."	"They [the youngsters] cross a [makeshift] suspension bridge, risking their necks and those of other citizens."

In the first example, there is no mention in the wrong translation of the "agent" (the "doer" of the act of blowing up the bridge), i.e. the Germans, whereas in the Russian original this was clearly specified, albeit in an inverted construction. In the second example, there are actually two case errors in the wrong translation. The first is the misrepresentation of

"other citizens" as the object of "risking"; the second is the omission of "the citizens" as subject of "cross" ("the bridge" is, of course, omitted here, too, but our grading practice is to assess no more than 8 points per sentence. This and other general grading procedures will be discussed under "General Observations" below).

The two examples above are instances of mis-translation within the framework of simple noun-verb relations. We also assess 4 points for interclause errors which usually involve mis-placement of relative (i.e. adjectival) clauses or adverbial clauses and which impair relations in meaning between clauses or sentences. One example (from a Russian text concerning a method of chemical analysis:

<u>Correct translation</u>	<u>Wrong translation</u>
"It is true that it is an expensive but proven method. However. . ."	"The method is expensive but, in truth, well tested. But. . ."

"It is true. . ." must govern the entire sentence, especially as the sentence is to be contrasted with the following sentence beginning with "However. . ." The misplacement of the initial phrase is thus a 4-point error.

A second example is more complex. In this case, also involving Russian, the original text had a somewhat unusual conditional construction which covered two sentences:

<u>Correct translation</u>	<u>Wrong translation</u>
"If the ore is good, a mine can be constructed. If it is worthless, you can search further."	"Good-you can build a mine, but it isn't suitable to look for another."

Here we took off 4 points for the wrong relationship between "good" and "you can. . ." resulting from the failure to translate the "if" clause. We did not give a double penalty for the omission of the second "if" but we did deduct another 4 points for an incorrect collapsing of ". . . it isn't [good], you can. . ." into one clause.

A final example is a case of appositional agreement in Japanese:

<u>Correct translation</u>	<u>Wrong translation</u>
"The North Korean Foreign Minister met again with the Foreign Minister of Peru [which is] the sponsoring country whose position is said. . . ."	"The North Korean Foreign Minister met again with Peru's Foreign Minister, (who is said to be close to South Korea's side) in the host country."

Failure to put the clause in the right slot cost the person taking the test 4 points.

UNCLASSIFIED

Dozens of other examples could be easily cited but the above should give some idea of syntactic error (I might note in passing that in our experience few people pass who make more than two such errors).

2.3 Lexical errors (2 points each)

The term "lexical" is something of a misnomer here because the error type covers not only incorrect vocabulary items but also certain prefixes and suffixes which are usually associated with syntax but are in fact more easily treated independently of syntactic relationships. Mistranslating, say, the German *die Strasse*, "the street," as "the apple" would obviously be a glaring error but it would not as such affect the *syntax* of the sentence. The same can be said of mistranslating the plural form *die Strassen* as "the street," or of rendering the future tense of a verb as a past.

We have coined an admittedly awkward phrase, "punctilinear error," to cover both kinds of 2-point errors. Such an error can be discerned at a given point in a "line" or string (hence the name) without the need for syntactic analysis. Below are some examples of punctilinear error:

<u>Correct translation</u>	<u>Wrong translation</u>
"There were only suppositions; no one knew for sure whether there was any ore [in the prospecting area]."	"There were only suggestions; no one knew . . ."
"The . . . mine is located near the city of. . ."	"The mine is located next to the city of . . ."
"It is a very rich mine."	"It is the richest mine."

The first two errors clearly involve vocabulary errors, while the third reflects a misunderstanding of a point of grammar (relative vs. absolute degree of superlative); in none of these cases is it very difficult to determine that a 2-point error has been made. In another instance the judgment is more difficult: a phrase which should have been translated from Russian as "the beloved home team" was rendered as "the favorite local team." The latter phrase can be understood as synonymous with the former, or it can be read as "the favorite (of several local teams)." Although 2 points could be taken off here, it would seem more reasonable to take off one, the penalty for a violation of English usage which I will now discuss.

2.4 Errors in English usage (1 point)

Admittedly questions of usage and convention are to a degree subjective, and it has been our experience that what is awkward or strange to one person may not offend another in any way. Hence we usually assess one-point errors only

when there is consensus among the graders. There are enough such cases, however, to make the one-point error a major factor in the final grade. Some examples appear below. The first example is a sentence concerning repair of a bridge:

<u>Idiomatic translation</u>	<u>Stilted translation</u>
"No one has put his hand to [restoring] the bridge."	"By no means have somebody's hands touched the bridge."

The "English" in this case is so poor that any grader would deduct at least one point, regardless of possible major errors in the string. In most cases, though, the strings are not as long. Let us consider a few less-extended cases:

A test taker writing about mine excavation translated a phrase as ". . . dug one drill hole . . .," an action impossible by definition, although the general meaning is clear. (Poor usage of this kind is often the result of a translator's adhering too closely to the original language forms.) Another used the nonexistent phrase "to his luck" in the sense of "luckily for him"; a third came up with "It completely won't do" for "It won't do at all." The list could from our experience be extended indefinitely.

Finally, we take one point off for English words and phrases which, while not in themselves awkward or peculiar, violate conventional usage. For example, translators who stick closely to original language forms will render "Secretary of State Kissinger" as "Foreign Minister Kissinger," or the "Pacific Ocean" as the "Quiet Ocean." When we feel that a personal or geographic name should be known to any literate person, we will deduct a point if a test subject misrepresents it.

2.5 Spelling and punctuation

Nothing is taken off for orthographic mistakes unless they will likely lead to misunderstanding, in which case the appropriate points are deducted.

3. General guidelines and caveats

3.1 Recurring errors

We try as hard as possible to avoid taking off points each time the same error is made. This is not too difficult in the case of lexical items, for once a translator decides that a word meaning "general" should be translated "field marshal," he will usually be consistent. Much the same is true of violations of English convention such as "Foreign Minister" for "Secretary of State." Repetitions of syntactic errors are much more difficult to spot; in cases where we are unsure whether the identical error has been repeated, we assess an additional 4 points.

UNCLASSIFIED

3.2 Double jeopardy

A double error over an identical stretch of text is penalized only at the higher rate. Thus, if the translator not only incorrectly reverses the order of "dog bites man," but in addition misidentifies the animal ("man bites cat"), he loses 8 points for the two syntactic errors but nothing for the vocabulary mistake.

3.3 Importance of context

We are careful in judging errors, particularly of the 2-point variety, in terms of context, and we try to avoid relying on dictionaries as final arbiters in every case. Thus, the sentences "He doesn't have *the* money to go" and "He doesn't have *enough* money to go" mean approximately the same thing, but no dictionary will ever inform us that "the" means "enough," or vice versa. Similarly a bilingual dictionary, particularly a limited one, cannot give enough translation choices to cover every situation. Hence the "literal translation" monstrosities that are docked one point (and sometimes 2 or even 4 points).

3.4 Need to distinguish between language forms and language as used

One of our major problems from the time the grading system was put in effect has been the tendency on the part of some graders to consider the *forms* of language as somehow equivalent to the *effects* of utterances. That is, they will protest, for example, that the omission of a negative particle in a translation can as seriously affect the meaning of the passage as, say, an error in verb-noun relationships, and will insist that the same number of points should be docked for each.

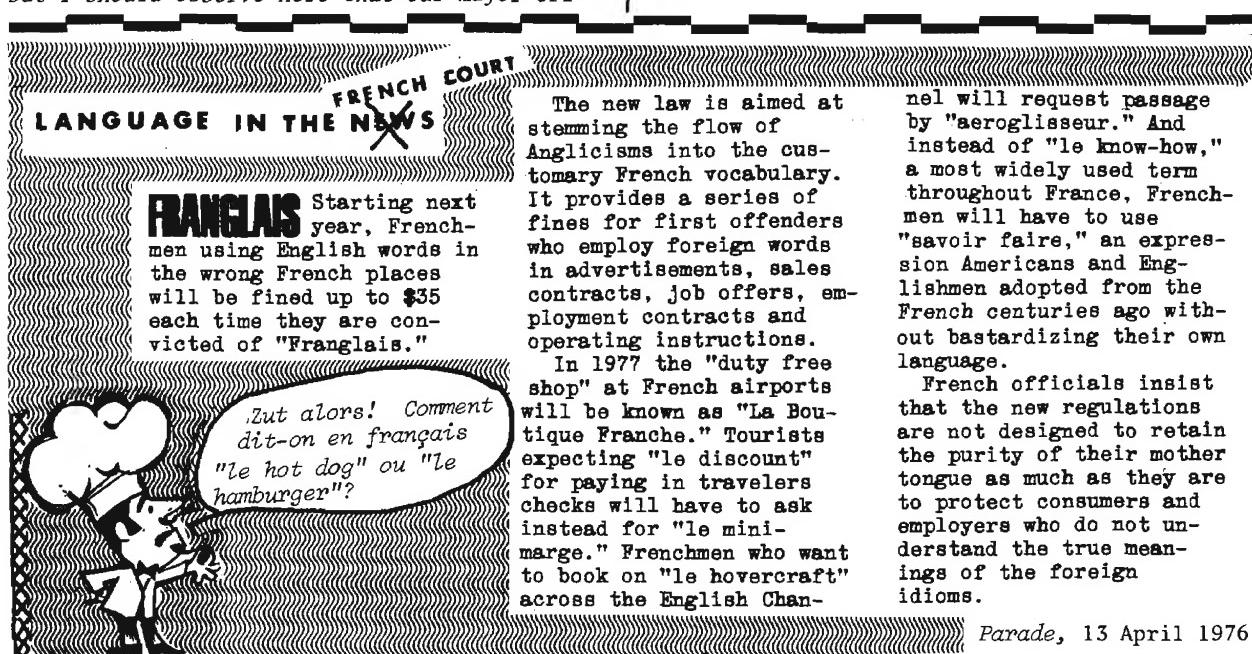
This attitude is of course very understandable, but I should observe here that our major cri-

terion for grading is syntax, which is to say the relationships among the elements of the sentence (what things go with what other things, and in what way), and the minor criteria relate to word choice and usage. This division is admittedly reminiscent of training and the classroom rather than language used in everyday life. Yet these are the criteria which have been used in the teaching of foreign languages and with which subjects and graders alike are most familiar. Furthermore, it would be extremely difficult, perhaps impossible, to devise a grading system according to which certain kinds and "strings" of information are considered more important than others; nor is such an approach needed for beginning translators. We have found that natural texts, not contrived ones, are best used, but the criteria by which the translations are judged should be formal, of the kind described above. They cannot be gut reactions to (mis)information.

3.5 Procedures to aid reliable and valid grading

As a final observation, we have found a tendency among some graders to temporize, especially in docking a paper 4 points, if they feel that the underlying cause of a mistake was a simple misunderstanding of a single word or grammar form ("I can see how he arrived at that"). This is unfortunately a kind of mind-reading that may be invalid and is certainly unreliable, since no two people draw the same kinds and numbers of inferences. The only thing we can judge is the syntactic and lexical rightness or wrongness, and the English usage, present in each paper.

(UNCLASSIFIED)



INTEGRATED ANALYSTS

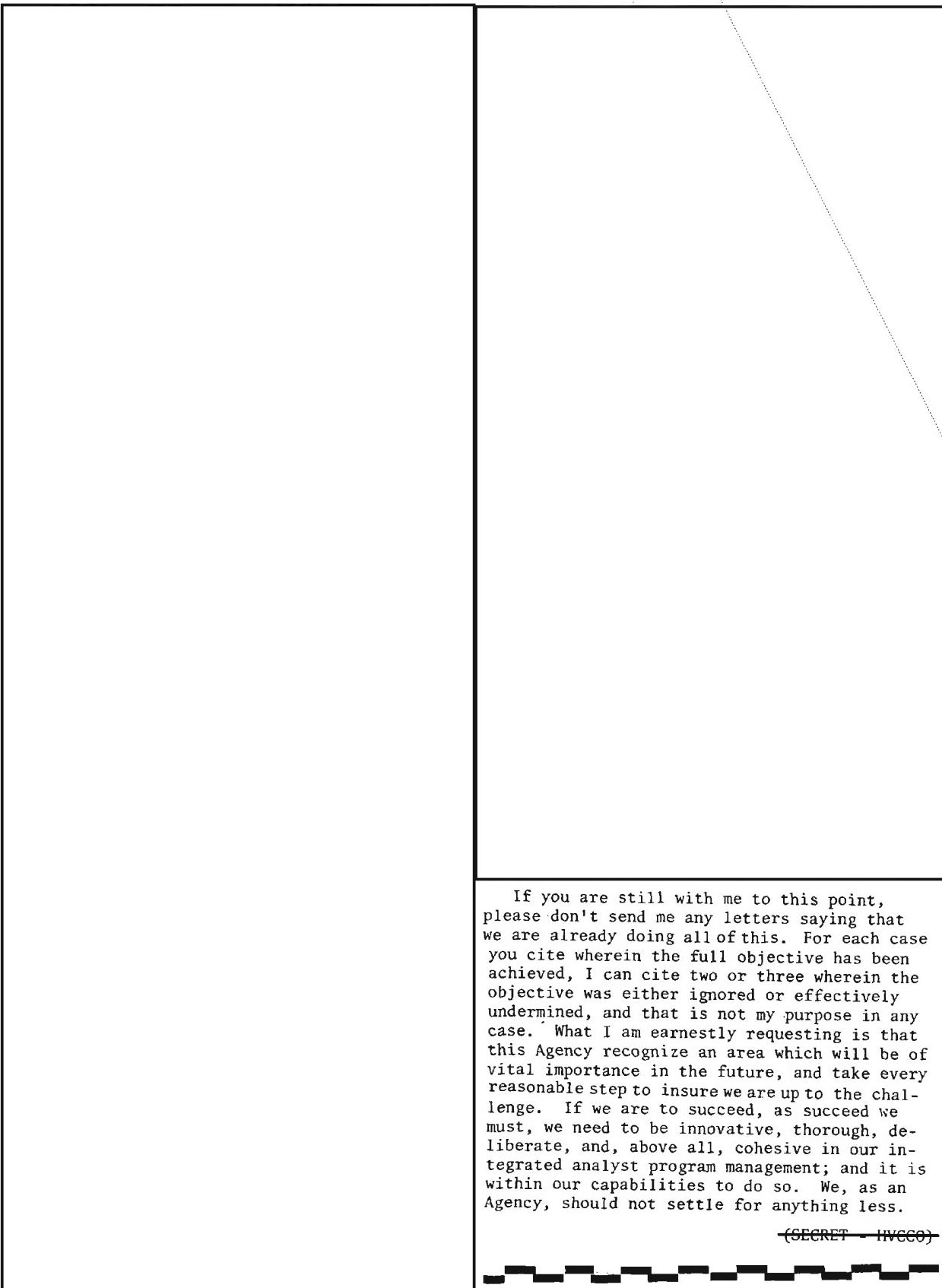
SEPTEMBER		MARCH		SEPTEMBER		MARCH		SEPTEMBER	
APPLY	1 2 3 4	6 7 8 9 10 11	12 13 14 15 16 17 18	18 19 20 21 22 23 24 25	26 27 28 29 30	FOR ASIA	LESSON	KIDS	OPERATION
6	(6) 7	8 9 10 11	12 13 14 15 16 17 18	18 19 20 21 22 23 24 25	26 27 28 29 30			1 2 3	1 2 3
12	13 14 15 16 17 18	18 19 20 21 22 23 24 25	26 27 28 29 30					4 5 6 7 8 9 10 11	4 5 6 7 8 9 10 11
18	19 20 21 22 23 24 25	26 27 28 29 30						11 12 13 14 15 16 17 18	11 12 13 14 15 16 17 18
24	25 26 27 28 29 30							19 20 21 22 23 24 25	19 20 21 22 23 24 25
30								26 27 28 29 30	26 27 28 29 30

FOR ASIA

A COHESIVE APPROACH

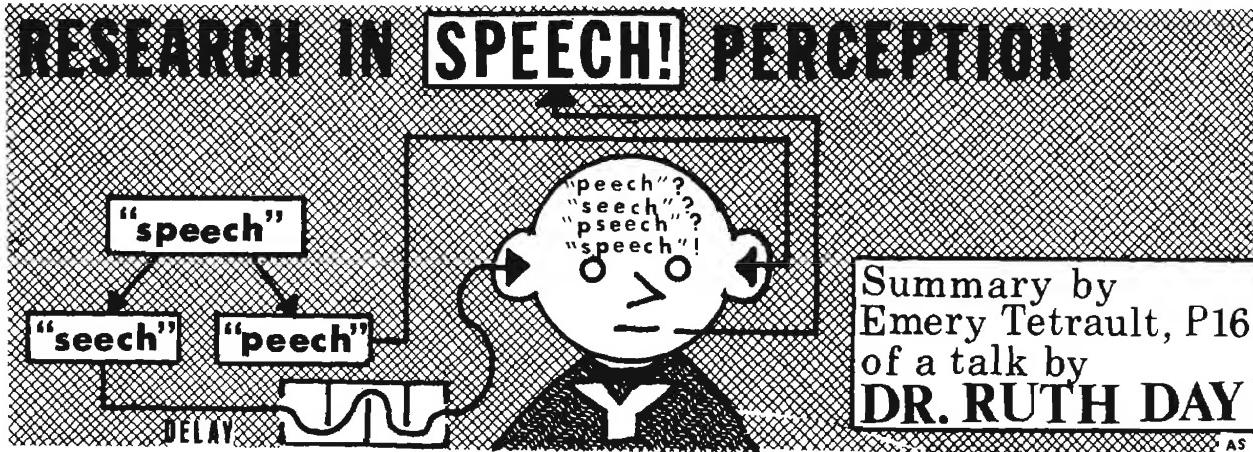
P.L. 86-36

On the other hand, in spite of the resource decrement, the intelligence requirement continues. SIGINT remains our first line of defense, and it is incumbent upon us to respond to this charge with all the resourcefulness we can muster.

~~SECRET~~

If you are still with me to this point, please don't send me any letters saying that we are already doing all of this. For each case you cite wherein the full objective has been achieved, I can cite two or three wherein the objective was either ignored or effectively undermined, and that is not my purpose in any case. What I am earnestly requesting is that this Agency recognize an area which will be of vital importance in the future, and take every reasonable step to insure we are up to the challenge. If we are to succeed, as succeed we must, we need to be innovative, thorough, deliberate, and, above all, cohesive in our integrated analyst program management; and it is within our capabilities to do so. We, as an Agency, should not settle for anything less.

~~(SECRET - HVECO)~~



The subject of individual differences in speech perception has not been a burning issue, either in cognitive psychology or in psycholinguistics, but it could be of intense interest to anyone who is responsible for selecting and training voice linguists. This was the main inference drawn from a talk given by Dr. Ruth Day, of Yale University and the Haskins Laboratory, to SIGVOICE (the Crypto-Linguistic Association's Special Interest Group on Voice). Her talk was enthusiastically received and considerable support was given at that time to the notion of following up on her findings. During the time that has passed since that talk, a few actions have been taken in the direction suggested. While NSA has not funded Dr. Day directly, RS4 has been supporting research in individual differences in speech perception at Haskins Laboratory for the past year. In addition, the Office of Naval Research has let out two contracts studying individual differences in speech perception, one with Dr. Day and one with the University of Oregon; RS4 has been receiving the progress reports from these ONR projects.

Dr. Day began by introducing the concepts of rivalry and fusion as demonstrated in experiments with visual stimuli through the use of a tachistoscope, a device which makes it possible to present different stimuli to each eye, and with auditory stimuli through the use of the dichotic listening technique.

One of the dichotic listening tasks was simply identifying input: did the subject hear "blanket" in one ear and "lanket" in the other ear, or did he hear the single word "blanket"? It turned out that subjects thus tested were either very good fusers (that is, they consistently heard a single word), or very good separators. There was almost no middle ground. This was particularly so when the outcome of fusion proved to be an actual English word, although the pattern was maintained as long as the result of fusion violated no English canon-

ical form (see Butcher in *NSA Technical Journal*, Special Linguistics Issue No. II).

Another task consisted of identifying the first sound heard when the two stimuli are presented with a slight time lag in onset (from 25 to 150 milliseconds). Everyone heard /b/ when "blanket" was given before "lanket," but part of the test population continued to hear /b/ first even when the onset order was reversed. Dr. Day advanced the hypothesis that this group was hearing only that which English permits -- /b/ followed by /l/. She called this group of people *language-bound*. The people who were capable of receiving and holding auditory stimuli in some kind of raw storage without immediately activating their grammar machines, she called *stimulus-bound*.

This bimodal or bactrian distribution of scores has been replicated with more or less randomly selected sample populations. In studies involving 100 Yale undergraduates, more than 90 were firmly identified with either one or the other group, and only five people showed no marked tendency toward membership in either the language-bound (henceforth LB) or stimulus-bound (SB) camp. Moreover, group membership appears to be stable. LB people do improve their performance by learning the task, but they never get to be as proficient at it as the SB types.

Dr. Day noted that the poor performance on this second task by LB people could be attributed to the fact that they simply can't make temporal-order judgments. However, when fusion of the two stimuli produces strings which are not canonically possible in English, then the LB subject does as well as anyone else in determining that (1) there are two stimuli and (2) one of them clearly precedes the other in onset time. Thus, when the stimuli are "back" and "dack," he has no problem making the temporal-order judgment, because neither "bdack" nor "dback" is a good candidate for an English morpheme. In other words, he can do the task in those situations where higher-order linguistic processing is ruled out.

UNCLASSIFIED

How do these two groups, once identified, fare on other kinds of tests? Do they retain their group identity? Dr. Day described some other tests which showed similar distributions.

Digit Memory

This warhorse of psychological testing usually produces a serial position curve. Test subjects have to remember sequences of digits and write them down in the same order as they were dictated. Items presented early and items which were last in the sequence tend to be remembered, but items in the middle are usually lost. This is what everyone expects and this is what all the methods of averaging and other obscuring individual differences give us. This is not, however, what SB subjects do. They make relatively fewer errors on this task than the population at large and the errors made occurred more or less evenly throughout the entire sequence. To get an SB subject to show the serial position effect, the task has to be made so difficult that the rest of the population finds it nearly impossible to do so.

Digit Memory with Zero Recall Cue

This task is the same as the previous one with one difference: each sequence ends with a zero, which is the cue for the subject to start recalling items. This procedure neutralizes the recency effect, at least for the LB types, but for SB subjects it affects not just the last items in the string, but all the items in the sequence. This, according to Dr. Day, suggests that there is something more than a quantitative difference between the performance of LB and SB subjects on this test. It supports the notion that the LB person has begun some immediate coding and longer-term storage of incoming auditory stimuli, while the SB type is holding the whole string in a kind of buffer memory. This is why the zero recall cue tends to affect the entire sequence for SB subjects.

Jotto

Given a target word -- say, "charm" -- and a list of comparison words, subjects are asked to find the one comparison word that shares the greatest number of letters with the target word. According to Dr. Day, the LB type will have a harder time with this task than the SB subject. He frequently underestimates the number of shared letters between target words and comparison words. He appears to be operating on the whole-word level and not seeing lower-order elements. With a target word like "sylph" and a comparison word like "prone," he would tend not to count the letter *p*, perhaps because he is going immediately from visual stimuli to phonemic representation (from *ph* to /f/).

Word Search

NSA Newsletter devotees immediately recognized this task since every month this esteemed

publication runs a puzzle consisting of words running every which way (actually, eight directions) in a matrix of letters. SB subjects did better than LB people when left-to-right directionality was violated. Dr. Day advanced the notion that SB types have the option of using both left- and right-hemisphere capability to solve tasks, while LB subjects are more or less locked into left-hemisphere -- i.e. linguistic -- processing.

Secret Languages

Dr. Day used a simple encode device to come up with one "secret" language: she transposed all /l/ and /r/ phonemes ("Maly had a ritter ram. . ."). Test subjects were asked to transform standard English (discrete words and then stereotyped connected discourse) into the secret language. She played some tapes of subjects performing this task. SB subjects were quite fluent, but the LB people had problems. One subject was almost pathetic as he tried valiantly to transform the word "bramble" and Dr. Day said she was going to spare us the pain of listening to his efforts against the name "Nelson Rockefeller."

Delayed Auditory Feedback (DAF)

The test subject wears earphones and talks into a microphone. His speech is fed back to him with a delay of about a fifth of a second. Again, Dr. Day played some demonstration tapes for us and, again, some subjects had little or no trouble with this task and others sounded like drunks in a nearly comatose state. Dr. Day herself was one of the subjects on the tape and we heard her trying, not altogether successfully, to recite the English alphabet (something which she assured us she knows). She noted that DAF performance is related to such tasks as foreign-language mimicry and phonetic transcription (in IPA or some comparable system) of unknown language forms.

*

Summary

So, we know that some people are language-bound and others are stimulus-bound and we have some notion of how to identify members of one or the other group. The immediate executive response ought to be, "All right, dammit, which one is the better one for a voice job?" Is it the LB who operates on a strong sense of linguistic expectancy, the anticipation of what can follow at every structural level from sound to meaning? Or is it the SB who can store raw auditory data in a short-term memory and more or less call things as he hears them? The answer to this question may not be as obvious as it seems on the surface, but it would certainly be worth the effort to push this research a little bit farther. We are in no position to pass up any help in the field of language processing.



NSA CRYPTOLOGIC COLLECTION

Have you ever visited the NSA Cryptologic Collection? Have you ever *heard* of it? If not, why don't you visit it? You'll be fascinated by what is contained in it. The collection is in Room 3W076, Operations Building, and is administered by [redacted] x4017s.

The collection is in a small room, but the room is crammed full of cryptologic literature of historical as well as completely up-to-the-minute value. Much of the collection is shelved in more than 1300 Shinn boxes, plus additional file-cabinet and shelf space. Much of the literature is unique and not represented in any other Agency collections (although the collection holdings are indexed in the NSA Technical Library, C5, records).

The collection contains historical documents pertaining to the use of cryptology in World War I and World II. In addition, it contains working aids of all vintages, pertaining to all aspects of cryptology, including a large number of cryptolinguistic working aids containing letter-frequency, word-pattern, and

other data derived from a broad spectrum of languages. A few samples are shown on the opposite side of this page.

Relative newcomers to the Agency who started late to save their back issues of the *NSA Technical Journal* can find a complete set here, back to Volume I, Number 1. (Incidentally, have you seen the special Twentieth Anniversary Issue of the *Journal* yet?)

The collection also includes a large number of open-source publications dealing with cryptologic subjects, including several rare books. And, of course, it contains a facsimile of the Voynich Manuscript? (You *can't* say that you haven't heard of the Voynich manuscript!)

With the exception of the rare books, most of the articles in the Cryptologic Collection can be borrowed. All the holdings are carefully cross-referenced, and [redacted] is always pleased to help you find what you are looking for.

P.L. 86-36

P.L. 86-36

(UNCLASSIFIED)

~~TOP SECRET UMBRA~~

...and the patterns in

...on of the book are alphabetized FROM RIGHT TO LEFT.

WORDS AND PHRASES
(pp. 1 - 130)

This section contains individual words and a few common phrases. This material may be used to attack any portion of a message. Each entry in th

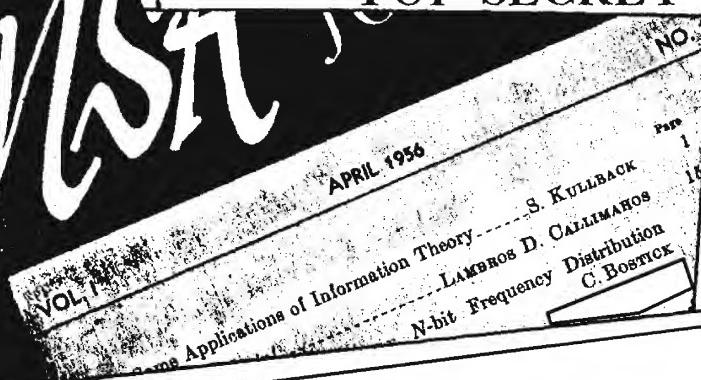
~~TOP SECRET EIDER~~

EO 1.4. (c)
P.L. 86-36

The main sources of material

1. Captured German documents, activities of agents in
2. Papers by Mr. Scott on + systems.

P.L. 86-36



EO 1.4. (c)
P.L. 86-36

~~TOP SECRET GLINT~~

~~TOP SECRET GLENT~~

August 76 * CRYPTOLOG * Page 18

~~TOP SECRET UMBRA~~

"LETTERS TO THE EDITOR ARE COMING!"

E.L. 86-36

PAUL REVERE'S RIDE TO NEW YORK

To the Editor, CRYPTOLOG:

There is a disquieting bias in Mr. David Gaddy's "On Being Truthful" (CRYPTOLOG, April 1976) which seems to want to pull "SIGINT equals truth" to the other side of the seesaw. To balance SIGINT's unsophisticated view of itself as being on the side of the angels, Mr. Gaddy points out intrinsic flaws in the SIGINT production process: sources might lie; some SIGINTers are more competent than others; the SIGINT facts suffer from interpretation; "sanitization and suppression" cause obfuscations; communications are susceptible to deception. He piles up the evidence until "SIGINT equals truth" slides to the other side of the fulcrum, where SIGINT is presented as inherently false.

What should we think, then, we SIGINTers? Is a SIGINT fact true? Yes. Emphatically, yes.

Certain basic principles underlie and guide any enterprise. In the SIGINT business one of these is that the lines of communications follow the chains of command. This means that organizations use electrical communications to systematically pass orders, requests, answers, plans, instructions, etc., and these communications speak for the organizations. Those lines of communications are not established to deceive us. That the SIGINT derived therefrom is true is really the only way to approach our profession.

Yes, letters to the editor (and articles, too) are still coming, in response to Vera Filby's article "How Do We Know It's True?" (CRYPTOLOG, February 1976). Take, for example, the following letter, which is in response to an article that was written in response to Mrs. Filby's article.

I am convinced of this; yet I would join Mrs. Filby and Mr. Gaddy in encouraging a deception study to determine its frequency and the conditions under which it would likely occur. The results are sure to reinforce the value of SIGINT and to allow quick reply to inquiring non-SIGINTers, who, understanding little of the nature of the SIGINT beast, are prone to worry about that aspect of it they do understand -- its potential for deception.

In all fairness, though, deception is not the main point of Mr. Gaddy's article. But what is the main point? Is it his summary idea encouraging continuing "education, indoctrination, and training" about the limitations of SIGINT? I do not think so, because that is certainly an easily acceptable idea that scarcely requires much rationale in its support. Main point aside, I think Mr. Gaddy's most important point is his allegation that we add falseness to

~~SECRET SPOKE~~

it not the professional SIGINTer? To use the bicentennial "VISINT" example now in vogue, should Paul Revere have dashed from house to house, giving his fellow-citizens a flee/no-flee option, thus: "Prearranged signals indicate British marching on a path that leads to our town"; then, in an aside, under this breath, "but don't blame me if you sacrifice a night's sleep and they never get here -- I'm just telling you what is reflected by the one-if-by land-two-if-by-sea signal." No. Paul Revere said, "To arms! The British are coming!" A cynical townsman -- at least one -- probably said, "What does that turkey know? I'm going back to bed." But, as we now know, there were few practicing cynics in those days; and, if any, they were probably doomed to obscurity because of it. History shows that Paul was believed. But why was he believed? Because he was trusted. He was a hard-working technician, deeply involved in his pursuits and well known for his competence -- he often provided fellow-citizens good counsel. The townspeople trusted him to understand what was going on and relied on his judgment.

Also, Paul was believed because his message was direct, unequivocal, forceful. Its point was not begged by passive constructions^EOndr. 4. (c) cheapened by apologetic phrases, nor clouded over by stereotyped redundancies. His message neither required nor encouraged further interpretation. The townsfolk heard, believed, and reacted. Likewise, SIGINT product would become more effective if our reporting faithfully adhered to these same principles. The suppression of evidence incidental to the SIGINT fact -- evidence whose lesser lights do more to divert attention than they do to illuminate truth -- rather than obfuscating the SIGINT fact, would help us present it in a professional manner. The suppression of nonessential data is not a burden to the reporter. It is, rather, a precept fundamental to the reporting discipline. It is good reporting.

V12

~~(SECRET SPOKE)~~

Mr. Gaddy replies:

P.L. 86-36

To the Editor, CRYPTOLOG:

Thank you for the opportunity to comment on
[redacted] letter.

I am afraid that his reaction demonstrates that the attitude I deplored is so ingrained in some of us that an attempt at redress -- moving the pendulum back to a neutral midpoint by reminding ourselves just what we're about -- is instantly construed as a swing to the opposite extreme. I intended to be "disquieting." My "bias," on the other hand, was toward objectivity: I was attacking attitudes, not SIGINT. The attitude I was specifically after is cocki-

After all, who is in the best position to judge the accuracy and validity of SIGINT? Is

~~SECRET SPOKE~~

~~SECRET SPOKE~~

P.L. 86-36

ness, "an unseemly air of intellectual arrogance." That was my main point, stated in the second paragraph. To develop it, I recalled the components of COMINT, not to illustrate "intrinsic flaws in the SIGINT production process," but as realities, as givens. Total, balanced recognition of these givens marks the SIGINT professional, not the sign over his desk saying "SIGINT doesn't lie." And it was the SIGINT pro's attitude that I so extravagantly praised.

Rather than rebut the strawman précis of my views advanced by [redacted] may I take issue with what he says about deception (which some readers may recall, was Mrs. Filby's original point). A mind closed to the likelihood of deception is a likely candidate for deception. The now universally recognized "basic principles" on which SIGINT depends are, at the same time, the cornerstones for a program of deception. We generally possess a high level of confidence that (in part because it is so difficult to pull off) deception will not be used or, if it is, that we will be smart enough to detect it. As long as that "high level" is not absolute, I share [redacted] attitude. I do not expect deception in the mass of normal, "peacetime" intercept, for example. On the other hand, I except a foe to be as wily as I would propose to be. Without citing October 1864 as an early example of enemy use of deception against the U.S. Army, I would commend to [redacted] (and other readers who have not delved into it) Brown's recent *Bodyguard of Lies*. The test of camouflage is not whether you see it, but whether you don't.

Finally, I must say that I am as puzzled over the Paul Revere story as when I first heard it used to construct some sort of analogy. It's a good example of signal communication, but loses

[redacted]
me at that point. Does the horse equate to CRITICOMM?

David W. Gaddy, D5

(CONFIDENTIAL - MVCCO)

So does Mrs. Filby:

To the Editor, CRYPTOLOG:

You have asked me to comment on [redacted] response to Dave Gaddy's response to my article on deception. My comment is, great! This is just the kind of discussion I wanted to start. And as in all good, lively, informed discussions, not only is the main theme developed, but also sidelights and subtleties and related aspects P.L. 86-36 emerge. This happened in both these responses as well as in those from [redacted] (May CRYPTOLOG) and [redacted] (June-July CRYPTOLOG). The next stage that we apparently all want to get to is the serious research into the facts of communications deception, to the degree that we can ascertain them. We know there has been deception [redacted] in North Vietnamese communications in recent years. Where else? Can't we get everything we know assembled for study? Then we can proceed to an evaluation of the extent and circumstances of deception, the possibilities of recognizing it, and the chances of missing it. Granted, to some extent, this is like research into psychic phenomena, in that it may be an effort to know the unknowable -- but at least we can learn something in trying.

Vera R. Filby, E12

(SECRET SPOKE)

EO 1.4. (c)

P.L. 86-36



SOLUTION TO NSA-CROSTIC No. 4

(CRYPTOROG, June-July 1976):

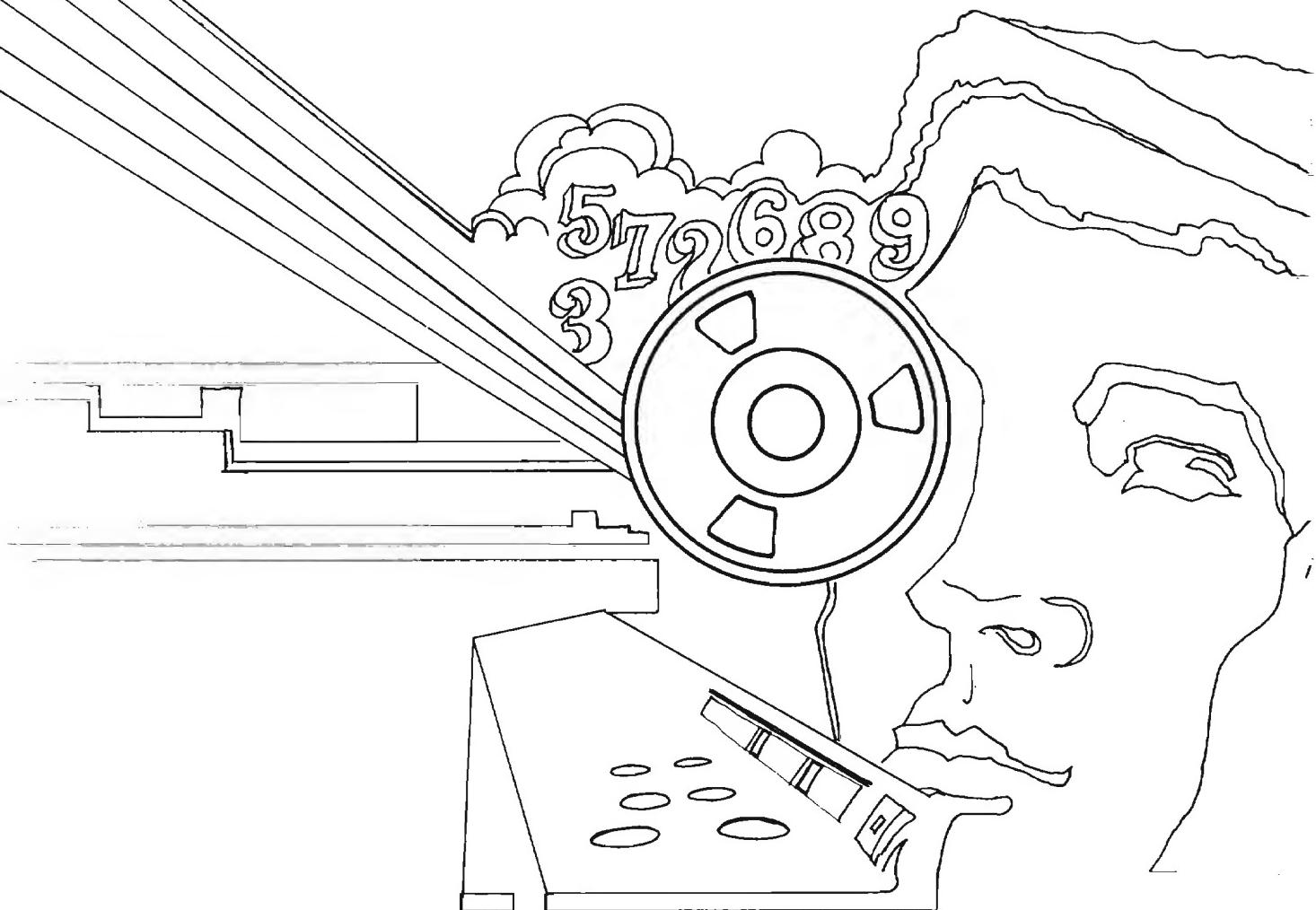
Jacob Gurin[-san], "[Employment of] Military Linguists,"

NSA Technical Journal, Vol. XIII,
No. 4, Fall 1968. (Also reprinted in
*NSA Technical Journal: Special Lin-
guistics Issue II.*)

"During the showing of a Japanese movie used as a training aid the students cheered mightily when, after about one hour of total lack of comprehension, they understood the maid when she knocked on the door and said 'Excuse me.'"

(UNCLASSIFIED)

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~